Multimedia Tools and Applications
https://doi.org/10.1007/s11042-020-10045-x

An efficient face anti-spoofing and detection model using image quality assessment parameters

Aditya Bakshi[1] · Sunanda Gupta[1]

Received: 1 May 2020 / Revised: 7 September 2020 / Accepted: 7 October 2020
Published online: 23 October 2020

Abstract

Biometric authentication poses a significant problem as reconstructed sample or fake self-manufactured samples used by intruders for accessing the actual real legitimate traits. The other prime concern for biometrics is the increasing demand for safety in mobile devices, such as smartphones and tablets etc. So, in the present scenario security for biometrics has gained considerable attention due to various inherent qualities of biometrics. For detection of valid user in a face recognition system with photographs, videos, and 3D models, face liveness detection system is a great technique against spoofing attacks for differentiating between the fake traits from the real traits. In this paper, a novel fake biometric detection technique utilizing liveness detection is proposed for detecting deceitful access attempts in the biometric face system. The prime objective of the paper is to propose a low-complexity fake biometric detection using different image quality assessment parameters i.e. Mean Square Error, Signal to Noise Ratio,SC etc. on the extracted features of the images. The authenticity of the proposed model is confirmed by analyzing the values of MSE, which are 5.8% and 8.49% more than the threshold value of nose and eye features. The same results have also been shown for other 11 different image quality assessment parameters. The experiments were done on the database prepared using the image samples of the 500 male and female students having age between 20 to 30 years.

Keywords Fake biometric detection · Image quality assessment · Liveness

✉ Aditya Bakshi
addybakshi@gmail.com

Sunanda Gupta
sunanda.gupta@smvdu.ac.in

[1] Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, Jammu, Kashmir, India

1 Introduction

In recent years, a biometric security system has evolved at a faster rate, and now it is turning out to be a broad area of research. With the arrival of mobile devices such as smartphones, the demand for biometric security has increased tremendously. In a traditional biometric security system, first biometric data are acquired through sensors, and then features are extracted from the received data samples. In the end, the acquired characteristics match with a set of templates in a database through matching modules. But in the present world, fake biometrics are posing a much more significant threat to the existing biometric systems. Different types of fake biometrics like printed iris image, masked face, and gummy finger are used to capture the behavior of genuine users to access the biometric system.

There are seven essential criteria for the biometric security system, as shown in Fig. 1 [23]. It comprises of uniqueness, universality, permanence, collectability, performance, acceptability and circumvention. Uniqueness and universality are generally used for identifying an authentic user among different groups of users. Deoxyribonucleic Acid (DNA) of any user is one of a unique parameter of a user that cannot be replicated. Permanence is one of the essential criteria in which every single characteristic or trait which ought to remain constant for a certain period of a person is recorded. These traits are then compared with the attributes in the database for identifying the fake biometrics. The criteria in which different characteristics are collected and verified are known as collectability criteria. Performance, accuracy, and robustness are the criteria that outline the working of the various security systems.

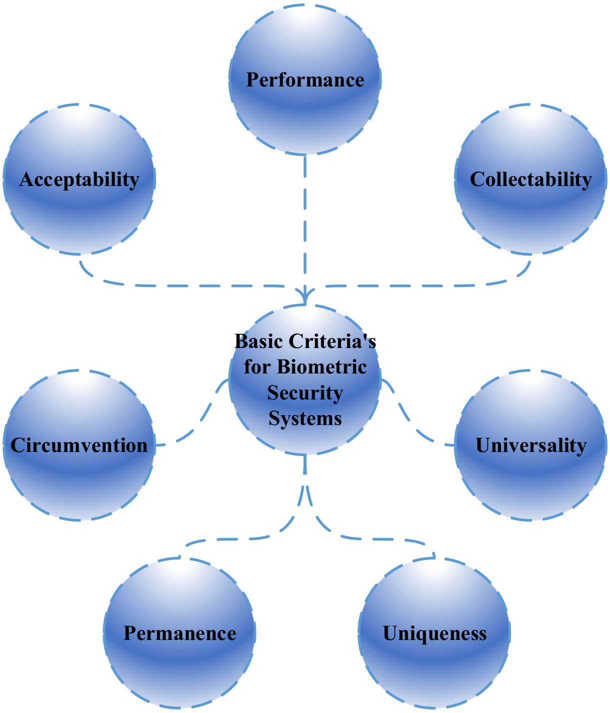


Fig. 1 Basic criteria’s for Biometric security systems

Acceptability criteria are judging whether the selected biometric security system is acceptable or not. Circumvention criteria are performing the verification process. It will decide the availability for each characteristic and trait of the user, which will help in checking the failures in the system.

Till 2020, a systematic categorization and comprehensive survey of anti-spoofing methodologies for face, iris, and fingerprint modality have been shown in Fig. 2. It summarizes various state-of-the-art methods in international competitions for examining the rate of detection. It also provides an outline of the anti-spoofing approaches for the face that are publicly available in different evaluated benchmarks. It reflects the improvement in the security level offered by the biometric systems against spoofing attacks and the further challenges to be faced for possible future research [4–6, 8, 14, 22, 25–28, 30, 35–40, 42].

Technologies are evolving, and so the security related to it. “Fingerprints cannot lie, but liars can make fingerprints” is an old saying which was very popular among the researchers in the past. This saying needs to be modified because now the intruders and spoof makers are making the spoofs of every biometric, which is available for use in the present technology [12].

Different technologies have taken different time for being evolved. Lots of development has been made in the field of biometric technology over the last forty years [3, 9, 17, 18]. For further improvement in the performance of the biometric systems, researchers from different fields have proposed different biometric techniques in forensics, on-line commerce, border surveillance, and access control [32].

New issues and challenges are very much resilient to specific external attacks that require a certain level of attention in the field of biometric recognition. It is also known that the use of biometric systems by the people in today’s life is growing year after year, as the positioning of biometric systems is increasing in different environments such as airports, laptops, or mobile phones.

Nowadays, it is elementary to get the knowledge for creating fake face mask, fingerprint, or iris. Lots of websites or tutorials videos are available that can be used to fool the biometric systems. This will make the general public aware of the flaws in the technology.

Various recognition systems are using the inherited traits, which are showing the inhibited characteristics for the biometric security system like face recognition system. Face recognition is a nonintrusive method for finding the discrimination of original images from the fake pictures. Facial recognition applications cover passive to controlled active verifications, from unrestrained identification of face, in a muddled background. For discriminating between real and fake images for the face recognition system, many approaches have been developed that cover the facial attributes such as eyes, eyebrows, nose, lips, and chin. The real and fake images can be differentiated by combining the number of canonical faces with the original images. This combined database of the images is used to verify the performance of the face recognition systems [9]. In the database, the number of restrictions is imposed for obtaining the facial images, like it requires the special illumination for face capturing or solid and simple background. In fact, under

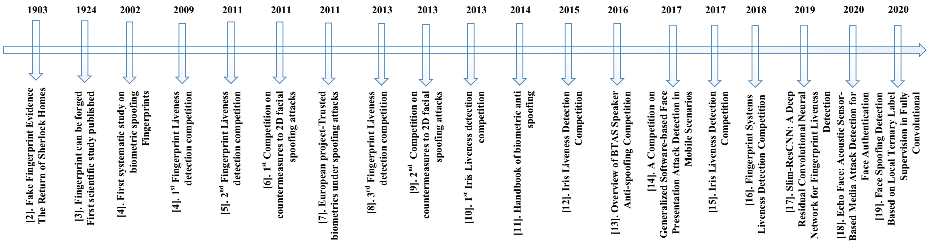

1903
[2]. Fake Fingerprint Evidence The Return of Sherlock Homes
1924
[3]. Fingerprint can be forged First scientific study published
2002
[4]. First systematic study on biometric spoofing Fingerprints
2009
[4]. 1st Fingerprint Liveness detection competition
2011
[5]. 2nd Fingerprint Liveness detection competition
2011
[6]. 1st Competition on countermeasures to 2D facial spoofing attacks
2011
[7]. European project-Trusted biometrics under spoofing attacks
2013
[8]. 3rd Fingerprint Liveness detection competition
2013
[9]. 2nd Competition on countermeasures to 2D facial spoofing attacks
2013
[10]. 1st Iris Liveness detection competition
2014
[11]. Handbook of biometric anti spoofing
2015
[12]. Iris Liveness Detection Competition
2016
[13]. Overview of BTAS Speaker Anti-spoofing Competition
2017
[14]. A Competition on Generalized Software-based Face Presentation Attack Detection in Mobile Scenarios
2017
[15]. Iris Liveness Detection Competition
2018
[16]. Fingerprint Systems Liveness Detection Competition
2019
[17]. Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection
2020
[18]. Echo Face: Acoustic Sensor-Based Media Attack Detection for Face Authentication
2020
[19]. Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional

Fig. 2 Momentous milestones in the evolution of Biometric Spoofing

different illumination conditions and different views, the face recognition system is facing a problem in recognizing a legitimate face from the captured images.

After identifying problems of face biometrics, it is observed that the biometrics for which the detection procedure is performed using an image is very efficient. In a picture, there are different image parameters based on which different image quality assessment (IQA) parameters are calculated. It is not feasible to cover all the image parameters for the detection procedure. In this paper, 12 IQA parameters have been used, which determines the desirable requirements for the liveness detection system.

1.1 Motivation

According to the literature study, there had been very little study on the use of liveness detection and IQA parameters simultaneously. Therefore, a robust anti-spoofing mechanism for face is the need of the hour. So, the main motive is to make use of the technique with distinct nomenclature on IQA parameters and results explanation through control of diverse valuation metrics. The other highlighting feature of the study is detection of real and fake users under different illumination conditions to identify the imposter who is making use of fake environment. .

1.2 Scope of the study

This section provides a brief introduction to the work that is already done on the fake face biometric detection to date. Gang Pal et al. [31] proposed a method for detecting photograph spoofing in face recognition by identifying impulsive eye blinks of the human eye. The proposed method is using a liveness detection approach with pictures are taking from generic web camera. The blink detection is articulated by taking conditional photographs from any direction and efficiently observes the whole working from data. Minh Hoai Nguyen et al. [29] presents different layers of human faces, such as a layer for other permanent facial features, a layer for glasses, and a layer for the beard. As it could be challenging to perform the modeling of the face with a linear subspace model, for easy modeling and modification of some specific structures layer separation method gives good results. For proper face synthesis and editing, the author presents a novel approach for automatic layer extraction for the detection of users. Gaurav Goswami et al. [15], explored a face recognition-based CAPTCHA for potential or high-level attacks. To comprehend the CAPTCHA, clients should effectively discover one set of human face pictures that have a place with the same subject, inserted in the complex background without choosing any non-face picture or impostor pair. The proposed calculation creates a CAPTCHA that offers better human accuracy and lower attack rates contrasted with existing methodologies. V. Ravibabu et al. [33] focused on a novel approach for the face recognition system by analyzing the current mechanisms for authentication on mobile phones securely and conveniently. This can be achieved by acquiring images with different angles of face data of the user and analyze the liveness detection of the user by contrasting and biometric format of information obtained in a database. The outcomes to the user face recognition are promising in liveness detection and dependable against spoofing. Daniel F. Smith et al. [34] identifies a technique binary watermark of captured video to address replay attacks for a face recognition system. Here, videos are captured using several cameras that are validated under different lighting conditions. Table 1 presents a summary of pre-existing work and their differences with the proposed method.

Table 1. Comparative Analysis of pre-existing work on Fake Biometric Detection with the proposed method

Ref	Liveness Detection	Extracted Features			Haar Wavelet Transformation based IQA parameter
		Face	Eye	Nose	
[31]	Yes	✓	✓	×	No
[29]	No	✓	×	×	No
[15]	No	✓	×	×	No
[33]	Yes	✓	×	×	No
[34]	No	✓	×	×	No
Proposed Method	Yes	✓	✓	✓	Yes

1.3 Contribution

- Building a model to detect the counterfeit biometrics using the proposed fake biometric detection method and validate the results using different IQA parameters.
- To best of our knowledge, an aliveness detection technique for detecting a fake biometric user is proposed. In this technique, the viola jones algorithm is used for recognizing a valid user using feature extraction in terms of face, eye, and nose. In the proposed model, different IQA parameters are used for detecting a fake biometric.
- A threshold is calculated which is decided for the valid user. If the coming user who is applying its biometric has not been able to obey the condition of the set threshold, the fake biometric is detected. But, there is a disadvantage of using different IQA parameters. By implementing different IQA parameters, the precision of identifying a fake biometric will increase, but it will decrease the processing speed, and thus, the system will become slow.
- Demonstrating the results for maintaining the high precision of detecting fake biometric with increased processing speed and a new IQA parameter has been proposed, known as Haar wavelet transform or WME (Wavelength based multi-scale entropy i.e. the local gray scale distribution of the pixel in an image and the multi-scale variation of texture information from different scale).

1.4 Organization

The organization of the paper is as follows. Section I provides the introduction and history of biometrics. In Section II, we discuss various image quality measures. In Section III, we discuss the proposed mechanism for detecting fake users. In Section IV, the simulation results of the proposed work are analyzed. Section V concludes the paper. The structure of the paper is as shown in Fig. 3.

2 Image quality measures

Image quality measures are the prime foundation stones for detecting the fake biometric images. These measures are applied to the pictures, and the originality of the image is analyzed based on different image features like sharpness, luminance level, and local artifacts, information gathered from two separate photographs and physical alterations or natural appearance [16].

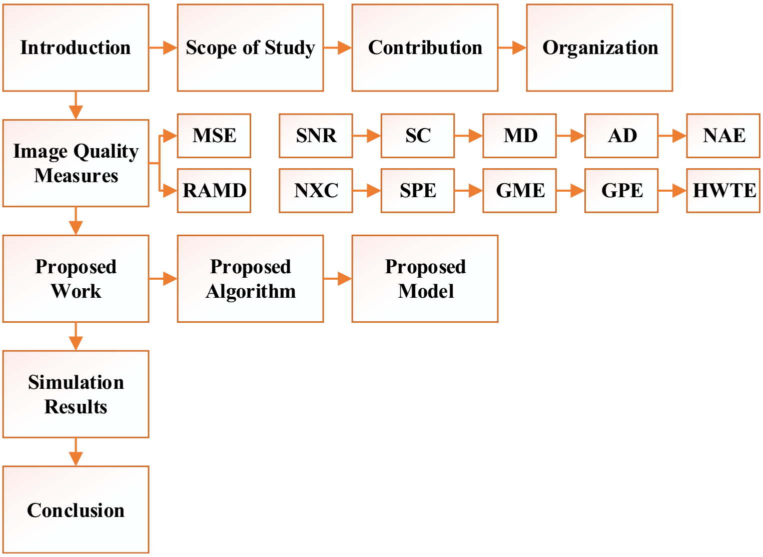


Fig. 3 Organization of the Survey

For detecting the fake biometric samples, different recognition systems are proposed, but there are some loopholes in each system like, irises images are likely to out of focus or blurred due to vibration in a picture when it is captured from a printed paper; face pictures will probably be over- or under-exposed if obtained from a mobile device; and fingerprint images present local acquisition artifacts such as spots and patches that captured from a gummy finger which is made up of silicon. Furthermore, the fake sample that is synthetically produced from an original sample that can be injected into the communication channel will miss some of the properties that can be easily detected in authentic images [13].

Following this "quality-difference" hypothesis, we explore the possible general IQA that are applied against different biometric attacks. General IQA methods can also be used to calculate the differences between fake and real samples [13]. IQA measures can be applied to any image to evaluate the given biometric modals for specific attacks. In the current state-of-the-art, many factors are there that support the use of IQA features for liveness detection. Image quality has been effectively used in the field of forensics, such as image manipulation detection [2, 41], and steganalysis [1, 24]. Image manipulation detection is a spoofing attack that covers capturing a picture of a facial image displayed in 2 Dimension devices (e.g., spoofing attacks with printed iris or face images). The different quality features of face images are shown in the present research work.

The previous studies that have been done in the field of forensic area, liveness detection for fingerprint and iris applications [10, 11, 20], featuring different trait-specific quality properties, have already been measured. However, in biometric systems, to measure the image quality of an image, various protection methods provide a reliable solution for liveness detection. For instance, in the detection of certain fingerprint spoofs, measuring the frequency of ridges and valleys may be a useful parameter for liveness detection of the fingerprint. But, this measurement is not helpful for the iris liveness detection method.

On the contrary to fingerprint spoof, in iris anti-spoofing mechanism, obstruction in an eye is valid to a more significant extent, but will not be helpful for fake fingerprint detection.

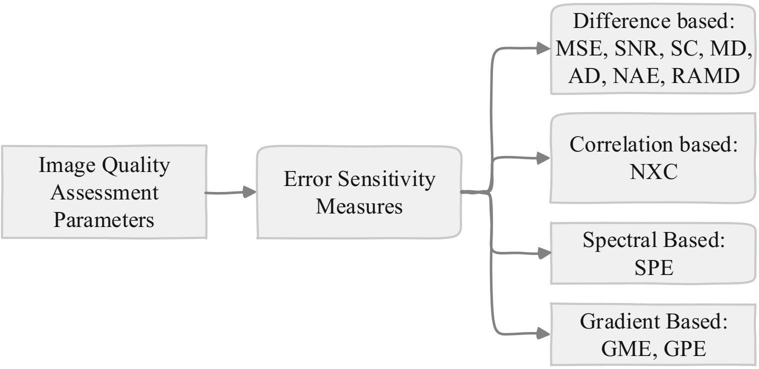


Image Quality Assessment Parameters
Error Sensitivity Measures
Difference based: MSE, SNR, SC, MD, AD, NAE, RAMD
Correlation based: NXC
Spectral Based: SPE
Gradient Based: GME, GPE

Fig. 4 Classification of IQA Parameters

Therefore, a certain amount of liveness detection methods follows the same reasoning that can be applied to the same state-of-the-art. All these good works provide awareness of the problems of spoofing detection. However, they are unable to specify various issues because spoofing attacks can be applied to one specific modality for detection purposes.

To discriminate between the samples of a real and fake image, the human observer often shows the different appearance of an original image. As stated above, the intended metrics and methods of IQA are used to estimate the appearance of human images in a perceive manner that is helpful for the liveness detection of spoofed attacks. IQA parameters are classified into four types, as depicted in Fig. 4. IQA parameters are used to access the test samples. It requires an undistorted reference image for estimating the quality of an image. Since this paper addresses the problem of fake detection, the input samples that are going to be accessed by the detection system in the form of an image should be used as a reference because it is unknown to the user.

The general representation of Fake biometric detection using Image Quality Measures is represented in Fig. 5. The first step in the process, as depicted in the figure, is to detect the user image using liveness detection. The second step applies the viola jones algorithm for detecting the features from the user's picture. In the targeted image, the feature extraction algorithm is used for extracting the face, eye, and nose from the image. The feature extraction algorithm is

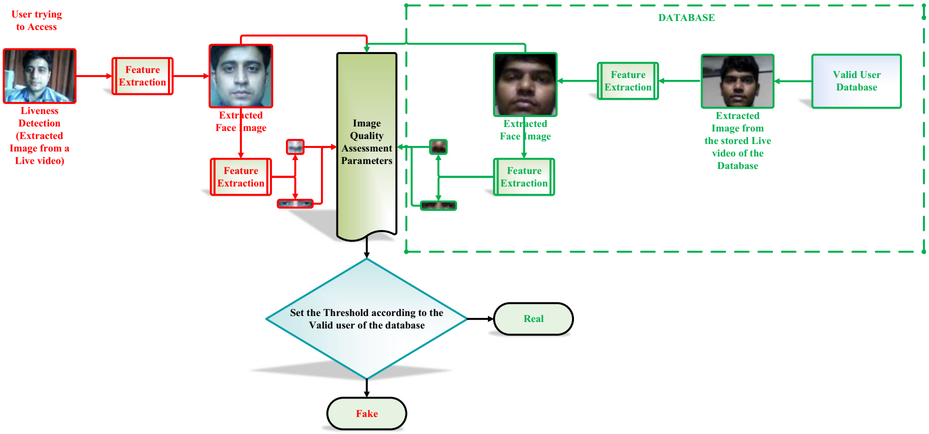

User trying to Access
Liveness Detection (Extracted Image from a Live video)
Feature Extraction
Extracted Face Image
Feature Extraction
Image Quality Assessment Parameters
DATABASE
Extracted Face Image
Feature Extraction
Feature Extraction
Extracted Image from the stored Live video of the Database
Valid User Database
Set the Threshold according to the Valid user of the database
Real
Fake

Fig. 5 General representation of Fake biometric detection using Image Quality Measures

also applied to the pictures of the database. In the third step, the extracted features images are applied for the IQA using different IQA parameters. In the fourth step, a certain threshold is selected based on the information of the valid user in the database. Based on the threshold, the authentication of the user is justified in terms of real or fake.

With the help of IQA metric, the quality between both the images (I and $\widehat{I}$) is computed for differentiating between the samples of real and fake biometrics having the size of N X M. The variables i,j in the below-mentioned expressions represent the pixel positions in an image [13].

2.1 Mean squared error (MSE)

The method of estimating the unobserved quantity of a sample is known as Mean Squared Error. To check the errors or deviations in the original sample, mean squared error calculates the average of the squares of errors in the original sample. MSE is an estimator that measures the quality of an authentic sample. The value for mean squared error is always non-negative.

For comparing the complete restoration of an original and fake image, mean squared error is required for measuring the quality of an image. The MSE between two images $I_{i,j}$ and $\widehat{I}_{i,j}$ is mathematically represented as:

$$MSE\left(I,\widehat{I}\right) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}-\widehat{I}_{i,j}\right)^2 \tag{1}$$

2.2 Signal to noise ratio (SNR)

The ratio of signal power to the noise power is known as SNR, which is expressed in decibels. It is used to compare the level of the desired signal to the level of background noise. SNR is used in imaging as a physical measure of the sensitivity of an image, as noise disrupts the quality of the original image. The mathematical representation of SNR is as:

$$SNR\left(I,\widehat{I}\right) = 10\log\left(\frac{\left(\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}\right)\right)^2}{N.M.MSE\left(I,\widehat{I}\right)}\right) \tag{2}$$

2.3 Structural content (SC)

The structural information content of an image is used to measure the sensitivity of an image by comparing the changes in the original image of the distorted image. The mathematical representation of SC is as:

$$SC\left(I,\widehat{I}\right) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}\right)^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(\widehat{I}_{i,j}\right)^2} \tag{3}$$

2.4 Maximum difference (MD)

Maximum Difference is used to measure the distortion between two images based on their pixel-wise differences. The mathematical representation of MD is as:

$$MD\left(I,\widehat{I}\right) = max\left|I_{i,j}-\widehat{I}_{i,j}\right| \tag{4}$$

2.5 Average difference (AD)

Average Difference is used to measure the *difference between the* measures of an *average value of the original image to the distorted image.* The mathematical representation of AD is as:

$$AD\left(I,\widehat{I}\right) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}-\widehat{I}_{i,j}\right) \tag{5}$$

2.6 Normalized absolute error (NAE)

The Normal Absolute Error is used to measure the average of absolute error from predicted (error) value to the real value. The mathematical representation of NAE is as

$$NAE\left(I,\widehat{I}\right) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left|I_{i,j}-\widehat{I}_{i,j}\right|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\left|I_{i,j}\right|} \tag{6}$$

2.7 R-averaged MD (RAMD)

R-averaged MD is used to calculate the average maximum difference. In this parameter, the maximum R number values are summed and divided by R, where R is the number of users. The equations that show RAMD is given by:

$$RAMD\left(I,\widehat{I},R\right) = \frac{1}{R}\sum_{r=1}^{R}max_r\left|I_{i,j}-\widehat{I}_{i,j}\right| \tag{7}$$

In the RAMD formulae, the value that shows r is the highest pixel difference between two images is illustrated by max_r.

2.8 Normalized cross-correlation (NXC)

For image-processing applications, the images can be normalized by varying the template and brightness of an image that arises due to lighting and exposure conditions. Normalized cross-correlation is represented in the form of an equation as,

$$NXC\left(I,\widehat{I}\right) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}.\ \widehat{I}_{i,j}\right)}{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(I_{i,j}\right)^2} \tag{8}$$

2.9 Spectral phase error (SPE)

Spectral phase Error can be calculated by taking the variance between the angles of Fourier transformed the original image to the angles of Fourier transformed reference image. It is represented in the form of an equation as given by,

$$SPE\left(I,\widehat{I}\right)=\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left|\arg\left(F_{i,j}\right)-\arg\left(\widehat{F}_{i,j}\right)\right|^{2} \tag{9}$$

2.10 Gradient magnitude error (GME)

Gradient magnitude error can be calculated by taking the variance between the gradient of the original image to the gradient of the reference image and averaged using the total number of pixels. It is represented in the form of an equation as given by,

$$GME\left(I,\widehat{I}\right)=\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(\left|G_{i,j}\right|-\left|\widehat{G}_{i,j}\right|\right)^{2} \tag{10}$$

2.11 Gradient phase error (GPE)

The gradient Phase error is the total number of pixels averages the variance between the angles of the gradient of the original image to the angles of the gradient of the reference image. It is represented in the form of an equation as given by,

$$GPE\left(I,\widehat{I}\right)=\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left|\arg\left(G_{i,j}\right)-\arg\left(\widehat{G}_{i,j}\right)\right|^{2} \tag{11}$$

2.12 Haar wavelet transform error (HWTE)

The grayscale digital image can be viewed as a matrix A of size M × N, whose entries are integers between 0 and 255, where 0 represents as black and 255 as white. The integer values that lie in between these two entries indicate a change in the degree of intensities of the gray image. Therefore, one-dimensional Haar wavelet transform $\widetilde{W}_M$ is applied on columns of A. Each column is transformed into two halves; the upper half gives a blur, and the lower half holds the differences or details in the data.

The processing of the rows of A can be done by multiplying $\widetilde{W}_M A$ by $\widetilde{W_N^T}$. This is done for defining the two dimensional discrete Haar wavelet transformation of the matrix A as $\widetilde{W}_M A \widetilde{W}_N^T$. The values of M and N must be integervalues.

$$\begin{aligned}\widetilde{W}_M A \widetilde{W}_N^T &= \left[\begin{array}{c}\widetilde{H}_{\frac{M}{2}}\\ \hline \widetilde{G}_{\frac{M}{2}}\end{array}\right] A \left[\begin{array}{c|c}\widetilde{H}_{\frac{N}{2}}^T & \widetilde{G}_{\frac{N}{2}}^T\end{array}\right]\\ &= \left[\begin{array}{c|c}\widetilde{H}_{M/2}\,A\,\widetilde{H}_{N/2}^T & \widetilde{H}_{M/2}^T\,A\,\widetilde{G}_{N/2}^T\\ \hline \widetilde{G}_{M/2}\,A\,\widetilde{H}_{N/2}^T & \widetilde{G}_{M/2}A\,\widetilde{G}_{N/2}^T\end{array}\right]\\ &= \frac{B|V}{H|D}\end{aligned}$$

In Fig. 6, the computation of matrix A has been done, in which, if A is partitioned into 2 × 2 blocks $A_{j,\,k}$, where $1 \le j \le M/2$, $1 \le k \le N/2$, the $(j,\ k)$ elements of B, V, H, D are constructed using the four values in $A_{j,\,k}$. Indeed, if

$$A_{j,k}=\begin{bmatrix} a & b\\ c & d\end{bmatrix}$$

Fig. 6 Representation of a Haar Wavelet Transformation

then each *(j, k)* element of B,V,H,D is

$$\begin{array}{cc} \frac{a+b+c+d}{4} & \frac{(a+c)-(b+d)}{4} \\ \frac{(a+b)-(c+d)}{4} & \frac{(a+d)-(b+c)}{4} \end{array},$$

respectively. In this way, the averages of the elements in the blocks $A_{j,\,k}$ can be treated as elements B and averaged differences as elements of V, H, and D in the vertical, horizontal, and diagonal directions, respectively.

HWTE is used for the recognition of an object from the digital image. A Haar-like feature can be generated by adopting Haar wavelets. It also requires the Viola-Jones method for extraction. The HWT is used to check the pixel intensities of each region (i.e., rectangular regions) of a specific location. The sum of pixel intensity values is taken, and the difference is calculated between them. The calculated difference will give the Haar wavelet transform error. It is represented in the form of an equation as provided by,

$$HWTE\left(I,\widehat{I}\right)=\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(\left|H_{i,j}\right|-\left|\widehat{H}_{i,j}\right|\right)^{2} \quad (12)$$

This can also be explained with an example; let us consider a database that has different images of human faces. Among all human faces in the database, the most common observation is that the region of the eyes is darker than the region of the cheeks. Therefore, a set of two adjacent rectangles that lie above the eye and the cheek region can be specified by Haar feature for face detection. The rectangles position is used to define the position of the face as a target object.

3 Proposed work

In today's expressive world, one of the significant concerns is providing security to the system. Since all the work is going on in the virtual environment, so security is the major problem for carrying out a virtual communication system. A biometric system is one such field that is robust to such security attacks. Biometric characteristics exist in the number of types and can be used in several applications. Each biometric has its own choice that depends on the application, and each of them has its strengths and weaknesses. The match between an application and a specific biometric can be determined by applying operational mode on the application and the properties of the biometric characteristic.

Different types of biometrics are commonly used for identification and verification of a particular sample like face, iris, fingerprint, gait, signature, and voice, etc. Each biometrics works on different functionality and has a different way of representation. This paper has focused on proposing a new fake biometric detection model using various features of the face in a lively environment.

Various models, such as iris, fingerprint, face, signature, and gait, are vulnerable to different types of fraudulent actions. Separate type attacks or threats have been analyzed for these fraudulent actions. But, one attack that affects the whole biometric community is spoofing or direct. In spoofing attacks, the intruder falsely accessing the biometric system by trying to mimic the behavior of the genuine user. Gummy fingerprinted iris image or face masks are some examples of spoofing attacks. As, the interaction with the device is done by using some regular protocols, but other digital protection mechanisms (e.g., encryption, digital signature, or watermarking) are not useful for these types of attacks. So, there is a need to develop and propose an efficient protection method against these types of attacks. The researchers around the globe are focusing on to improve the robustness and security level of the biometric systems by applying specific countermeasures for detecting fake samples from the real one and reject them.

Liveness detection techniques and anti-spoofing approaches that use different physiological properties have gained special attention from researchers and industry to distinguish between real and fake traits. For detecting the liveness of any sample, liveness detection methods are categorized into two techniques:

3.1 Hardware-based techniques

To identify the specific properties of a living feature (e.g., sweat on fingerprint, blood pressure, or specific reflection properties of the eye), the hardware-based technique uses the functionality of a particular device that is attached to the sensor.

3.2 Software-based techniques

In software-based techniques, standard sensors are used to detect the fake trait that has been acquired from the original sample (i.e., not from the characteristics itself but features of characteristics are extracted from the biometric sample to distinguish between real and fake traits).

For increasing the security of a biometric system, these two methods have advantages and drawbacks over one another and would be the most desirable protection approach, when combined. If the two techniques are compared, it is observed that the hardware-based schemes have a higher fake detection rate, but software-based methods require no new device, and its implementation is transparent to the user. Therefore, software-based techniques are less intrusive and less expensive. In the case of detecting many types of spoofing attacks, software-based technologies may be embedded in the feature extractor module, as they can operate directly on the acquired sample and not on the biometric trait itself.

The proposed model for fake biometric detection, as shown in Fig. 7, is being tested on different IQA parameters, as classified in Fig. 4. To organize the biometric sample as real or fake (i.e., the image acquired for the biometric recognition purposes are similar), requires only one input image. Image quality features operate on the whole picture of the user without searching for any specific traits. The biometric system does not require any preprocessing steps such as fingerprint segmentation, iris detection, and face extraction for computation purposes. The features generated by using image quality measures for a particular sample are operated by some simple classifiers for classifying it as real (created by a positive trait) or fake (synthetically produced). The computational load of the system is reduced with the use of distinctive image quality features. To extract a set of salient or discriminatory features, the biometric data (i.e., iris, face, or fingerprints) has to be processed by applying the feature extraction module. For example, in a fingerprint-based biometric system, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted by the feature extraction module.

In this section, an algorithm and flowchart representing the proposed efficient face anti-spoofing and detection model has been incorporated as shown below in Fig. 8. With the property of low complexity, this algorithm has been used to detect real and fake users. The IQA parameters have also been applied and the imposter image has been compared with the valid user database. The notations of the algorithm are explained in Table 2 that depicts the imposter user image, extracted features of valid user for face, nose and eye, IQA parameters and Threshold.

Algorithm for the Proposed Efficient Face Anti-Spoofing and Detection Model

```
1: Creating Database of Valid Users
$D = [I_1, I_2, I_3 \ldots \ldots I_N]$

2: Apply Voila jones algorithm for extracting the features.
$D_v = [D_f, D_e, D_n]$
$D_f = [I_1^f, I_2^f, I_3^f \ldots \ldots . I_N^f]$
$D_e = [I_1^e, I_2^e, I_3^e \ldots \ldots . I_N^e]$
$D_n = [I_1^n, I_2^n, I_3^n \ldots \ldots . I_N^n]$

3: Attack of an Imposter, $I_m$

4: Apply Liveness Detection to an Imposter, $I_m$

5: Apply Voila-Jones Algorithm on $I_m$ for feature extraction
$I_m \rightarrow I_m^f, I_m^e, I_m^n$

6: Apply IQA Parameters
$IQA = [IQA_1, IQA_2, IQA_3 \ldots \ldots IQA_{12}]$        //*$IQA_1 = MSE(I_1^f, I_m^f) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{1,ij}^f - I_{m,ij}^f)^2$ *//

7: Set the threshold for detecting the Imposter
$Th = [Th_1, Th_2, Th_3 \ldots \ldots Th_{12}$        //*$Th_1 = \frac{MSE(I_1^f, I_m^f) - MSE(I_1^f, I_1^f)}{2}$ *//

8: Detection of Fake Biometric
Initialize the IQA Vector
For i=1:1:12
If $IQA_i > Th_i$
Then $IQA_i = 1$
IQA = [IQA IQA$_i$]
End
i=i+1
End
If IQA is a Unity Matrix
Then Imposter is detected and blocked
Else
Valid User
End
```

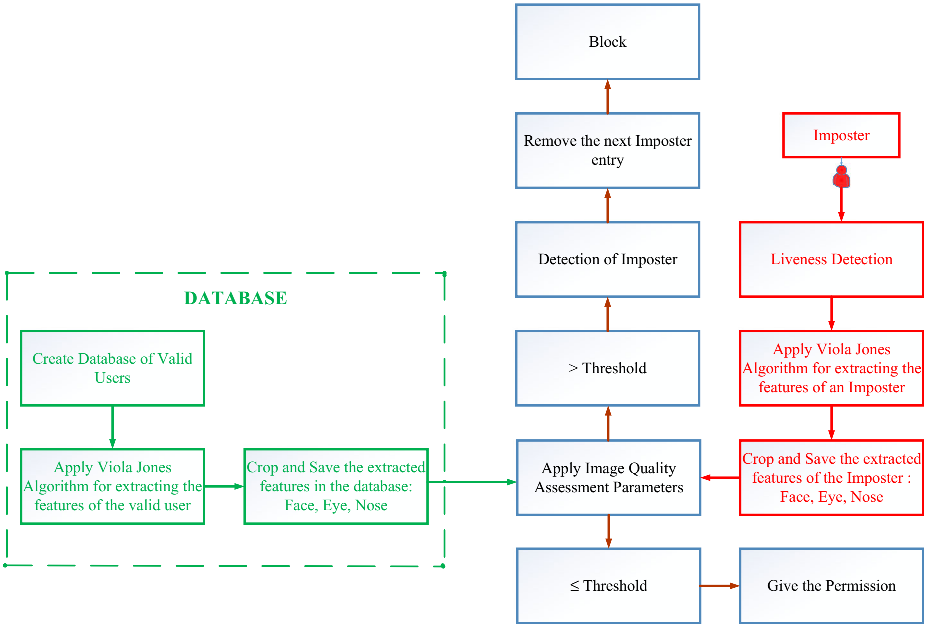

Block
Remove the next Imposter entry
Imposter
Detection of Imposter
Liveness Detection
DATABASE
Create Database of Valid Users
> Threshold
Apply Viola Jones Algorithm for extracting the features of an Imposter
Apply Viola Jones Algorithm for extracting the features of the valid user
Crop and Save the extracted features in the database: Face, Eye, Nose
Apply Image Quality Assessment Parameters
Crop and Save the extracted features of the Imposter : Face, Eye, Nose
≤ Threshold
Give the Permission

Fig. 7 Proposed Efficient Face Anti-Spoofing and detection model

4 Simulation results

After applying the proposed fake biometric detection method, different IQAs parameters are used for increasing the detection accuracy of the proposed method.

In this paper, the proposed low complexity model for the fake biometric detection is tested using different IQA parameters on the extracted images, for distinguishing the legitimate samples from the fake samples. The simulation results after applying the proposed method in terms of different IQA parameters are mentioned in Figs. 9 and 10.

It is clear from the Fig.9(a), that the MSE value of the legitimate user is 5.9% less than the threshold value, and the MSE value of a fake user is 2.4% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye, whose fake user's MSE value is 5.8% and 8.49% more than the threshold value, respectively.

It is clear from the Fig. 9(b), that the SNR value of the legitimate user is 8.2% more than the threshold value, and the SNR value of a fake user is 11% less than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's SNR value is 10.9% and 26.26% less than the threshold value, respectively.

It is clear from the Fig. 9(c), that the SC value of the legitimate user is 9.1% less than the threshold value, and the MSE value of a fake user is 5.5% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's SC value is 4.6% and 4.2% more than the threshold value, respectively.

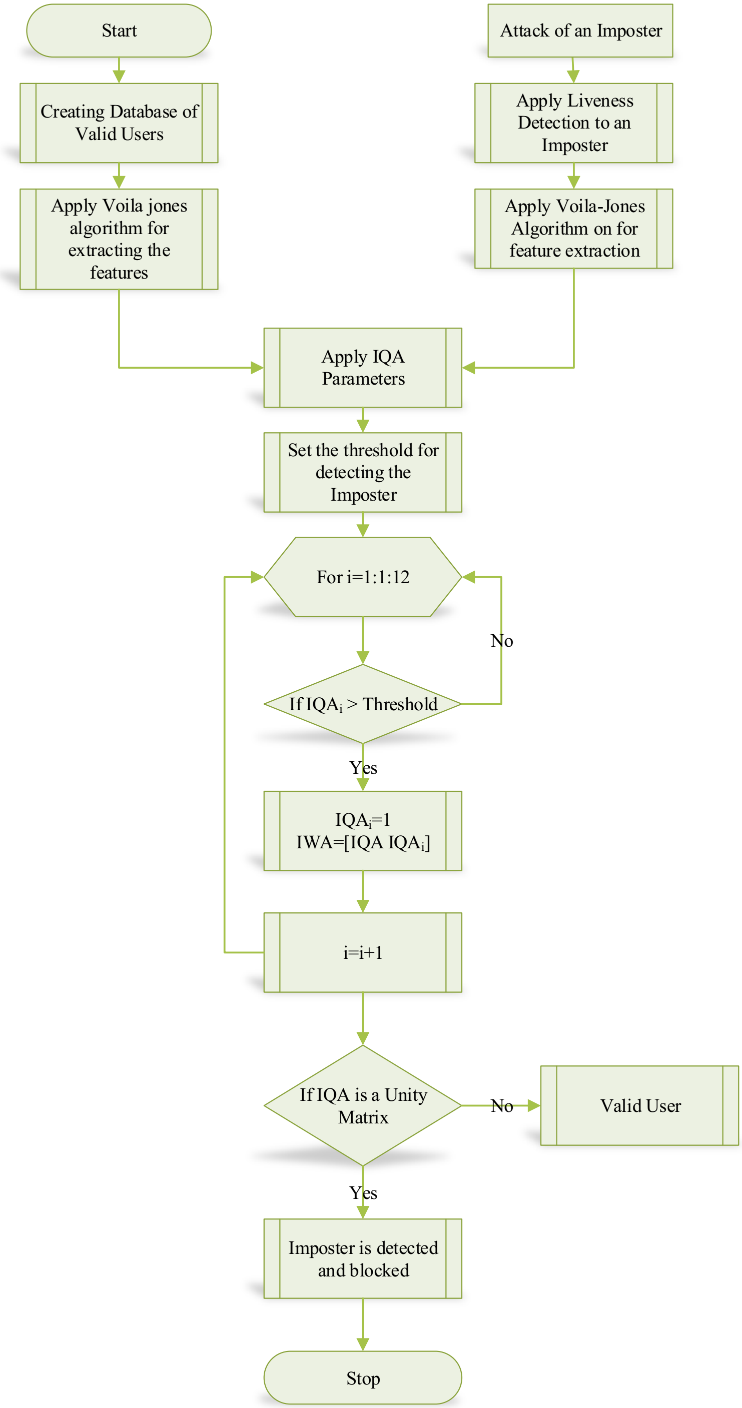

Start
Creating Database of Valid Users
Apply Voila jones algorithm for extracting the features
Attack of an Imposter
Apply Liveness Detection to an Imposter
Apply Voila-Jones Algorithm on for feature extraction
Apply IQA Parameters
Set the threshold for detecting the Imposter
For i=1:1:12
If IQA$_i$ > Threshold
No
Yes
IQA$_i$=1
IWA=[IQA IQA$_i$]
i=i+1
If IQA is a Unity Matrix
No
Valid User
Yes
Imposter is detected and blocked
Stop

Fig. 8 Flowchart for the proposed efficient face anti-spoofing and detection model

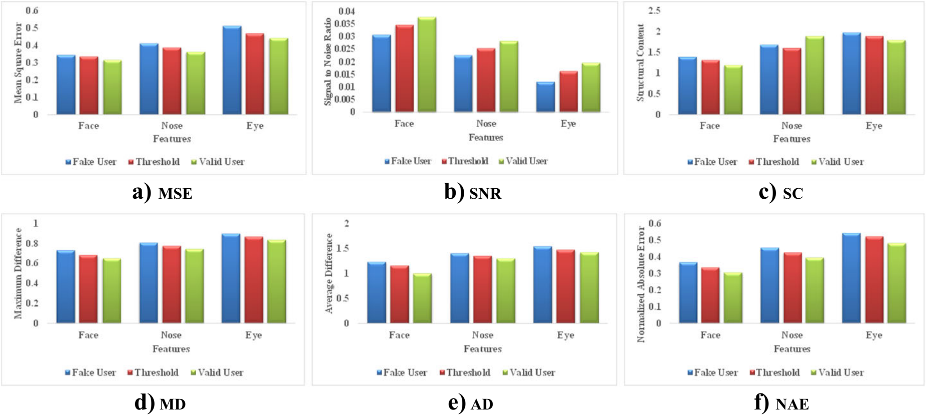
Table 2. Notations mentioned in the Algorithm

Notation	Description
D	Database of valid-user
I_1, I_2, I_3……I_N	Images of valid-user
D_v	Database of extracted features for valid users
D_f	Database of extracted features for the face of valid users
D_e	Database of extracted features for the eye of valid users
D_n	Database of extracted features for the nose of valid users
I_1^f, I_2^f, I_3^f…….I_N^f	Face images of valid users
I_1^e, I_2^e, I_3^e…….I_N^e	Eye images of valid users
I_1^n, I_2^n, I_3^n…….I_N^n	Nose images of valid users
I_m	Imposter user image
I_m^f	Imposter user face image
I_m^e	Imposter user eye image
I_m^n	Imposter user nose image
IQA	Image Quality Assessment Parameter
Th	Threshold

It is clear from the Fig. 9(d), that the MD value of the legitimate user is 4.6% less than the threshold value, and the MD value of a fake user is 6.5% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's MD value is 4.03% and 3.27% more than the threshold value, respectively.

It is clear from the Fig. 9(e), that the AD value of the legitimate user is 13.6% less than the threshold value and the AD value of a fake user is 5.9% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's AD value is 3.5% and 4.3% more than the threshold value, respectively.

It is clear from the Fig. 9(f), that the NAE value of the legitimate user is 9.06% less than the threshold value, and the NAE value of fake users is 8.3% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values



a) MSE **b)** SNR **c)** SC

d) MD **e)** AD **f)** NAE

Fig. 9 Simulation Results

of the nose and eye whose fake user's NAE value is 6.3% and 3.7% more than the threshold value, respectively.

It is clear from the Fig. 10(a), that the NXC value of the legitimate user is 3.9% more than the threshold value, and the NXC value of a fake user is 4.6% less than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's NXC value is 3.06% and 2.71% less than the threshold value, respectively.

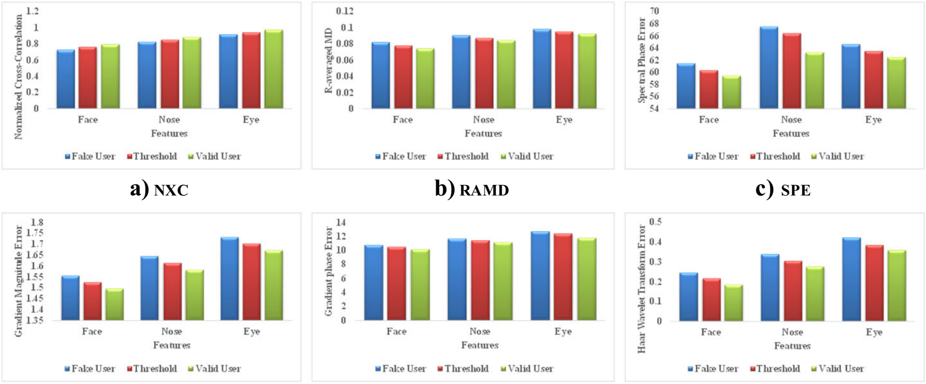
It is clear from the Fig. 10(b), that the RAMD value of the legitimate user is 4.6% less than the threshold value, and the RAMD value of a fake user is 4.98% more than the threshold value.

Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's NAE value is 3.96% and 3% more than the threshold value, respectively.

It is clear from the Fig. 10(c), that the SPE value of the legitimate user is 1.46% less than the threshold value, and the SPE value of a fake user is 1.85% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's SPE value is 1.65% and 1.71% more than the threshold value, respectively.

It is clear from the Fig. 10(d), that the GME value of the legitimate user is 1.93% less than the threshold value, and the GME value of a fake user is 1.90% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's GME value is 1.90% and 1.69% more than the threshold value, respectively.

It is clear from the Fig. 10(e), that the GPE value of the legitimate user is 3.19% less than the threshold value, and the GPE value of a fake user is 2.54% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics. The authenticity of the proposed model is confirmed by the values



a) NXC **b)** RAMD **c)** SPE

d) GME **e)** GPE **f)** HWTE

Fig. 10 Simulation Results

of the nose and eye whose fake user's GPE value is 2.05% and 2.5% more than the threshold value, respectively.

Haar wavelet transform error is used for the recognition of an object from the digital image. A Haar-like feature can be generated by adopting Haar wavelets and requires the Viola-Jones method for extraction. The HWT is used to check the pixel intensities of each region (i.e., rectangular regions) of a specific location. The sum of pixel intensity values is taken, and the difference between these sums can be calculated. The calculated difference will give the HWTE. The value of the HWTE of a valid user should be less than the absolute threshold value for recognizing a legitimate user, while the value of the HWTE of the fake user should be more than the absolute threshold value for detecting a fake user.

It is clear from the Fig. 10(f), that the HWTE value of the legitimate user is 14.47% less than the threshold value, and the HWTE value of a fake user is 11.76% more than the threshold value. Therefore, the result displays that the proposed fake biometric detection system is capable of detecting fake biometrics with high processing speed. The authenticity of the proposed model is confirmed by the values of the nose and eye whose fake user's HWTE value is 9.8% and 8.7% more than the threshold value, respectively.

5 Conclusion

Nowadays, the role of biometrics in the next generation system technologies has increased drastically. So, there arises a need for securing these systems. The fake Biometric Detection method is one of the steps towards this objective. In this paper, a fake biometric detection method has been proposed. The proposed method is using a liveness detection technique for detecting a fake biometric user. After applying the liveness detection, different IQA parameters are used for detecting a fake biometric. According to the nature of the image, based on the IQA parameter, a threshold is decided for the valid user. If the coming user who is applying its biometric has not been able to obey the condition of the set threshold, the fake biometric is detected. But, there is a disadvantage of using different IQA parameters. By implementing different IQA parameters, the precision of identifying a fake biometric will increase, but it will decrease the processing speed, and thus, the system will become slow. Hence, for maintaining the high precision of detecting fake biometric with increased processing speed, a new IQA parameter has been proposed, known as Haar wavelet transform. The proposed fake biometric detection method has been simulated using different IQA parameters. The simulation results in the paper display that the proposed method with different IQA parameters can detect fake biometrics. The value of the threshold is decided for each case by taking the average value between the values of the valid user and the fake user. The value of the threshold is then compared with the value of the fake user. If the value of the fake user is more/less than the threshold value, depending upon the IQA parameter, the fake biometric has been detected.

6 Future scope and applications

The challenges after observing the trends and results from the proposed model that should be addressed for solving the problems in this field that could help other authors in future directions.

Firstly, even though an efficient model for liveness detection is implemented on live images samples of the 500 students that produce great experimental results. But, results will be implemented by using other databases (i.e. LiveDet 2013) for achieving a promising and reasonable generalization [10].

Secondly, to solve the problem, we have implemented the techniques which give great results for the software-based liveness detection. As there are very large variations in the sensing methods, therefore, developing a hardware-based liveness detection method is difficult. So, a robust fake face toolbox could be required for developing hardware-based methods [7, 19, 21].

Finally, the performance of the liveness detection methods might be improved if some machine learning classifiers and more robust security mechanisms are used in field of health and medical. The work on a proper comparison between different classifiers will be taken into consideration.

The challenges can be hardware cost and complexity but it may be overlooked as the results after implementing this model are very robust.

6.1 Applications

The main authorities of the proposed model are that it can be used are following:

- Medical applications: Healthcare companies are using the concept of liveness detection for facial recognition for resolving the problems of frauds during the insurance claims. It is also helpful in taking care for patients in hospitals.
- Banking and Finance: A high quality of security for fraud prevention, banking and finance sector needs the use of liveness detection. To let customers securely log into their mobile banking apps, banks are already using facial recognition.
- Security: The use of anti-spoofing detection model for face is required to enhances capabilities of solutions like video security, access control and identity management systems.
- Governance: An accurate and safe identity of the users, a new step towards in governance system is introduced to eliminate of identity theft.

Authors' contributions The major author contributions are following:

Aditya Bakshi carried out the all research work and wrote this manuscript.

Dr. Sunanda has suggested some changes in formatting of the manuscript.

Compliance with ethical standards

Conflict of interest The author declares that there is no conflict of interest regarding the publication of this paper.

Data availability No data were used to support this study.

Code availability There is no significant code available for this paper.

Ethics approval Not applicable.

Consent for publication Yes. Consent has been given by an individual for the publication of their data or image.

References

1. Avcibas et al (2003) Steganalysis using image quality metrics. IEEE Trans Image Process 12(2):221–229
2. Bayram S et al (2006) Image manipulation detection. J Electron Imaging 15(4):041102–041102
3. Bledsoe WW (1964) The model method in facial recognition, Panoramic Research Inc., Palo Alto. CA, Technical Report, Technical Report PRI: 15
4. Boulkenafet Z et al (2017) A competition on generalized software-based face presentation attack detection in mobile scenarios. 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE
5. Chakka MM et al (2011) Competition on countermeasures to 2-d facial spoofing attacks." Biometrics (IJCB), 2011 International Joint Conference on. IEEE
6. Champod C et al (2014) Forgeries of fingerprints in forensic science. Handbook of Biometric Anti-Spoofing. Springer, London, pp 13–34
7. Chan PPK et al (2017) Face liveness detection using a flash against 2D spoofing attack. IEEE Trans Inform Forensics Secur 13(2):521–534
8. Chen H et al (2019) EchoFace: acoustic sensor-based media attack detection for face authentication. IEEE Internet Things J 7(3):2152–2159
9. Davis et al (1952) Automatic recognition of spoken digits. J Acoustical Soc Am 24(6):637–642
10. Galbally J et al (2012) Iris liveness detection based on quality related features." Biometrics (ICB), 2012 5th IAPR International Conference on. IEEE
11. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J (2012) A high-performance fingerprint liveness detection method based on quality related features. Futur Gener Comput Syst 28(1):311–321
12. Galbally et al (2014) Biometric antispoofing methods: a survey in face recognition. IEEE Access 2:1530–1552
13. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. IEEE Trans Image Process 23(2):710–724
14. Ghiani L et al (2013) Livdet 2013 fingerprint liveness detection competition 2013. Biometrics (ICB), 2013 International Conference on. IEEE
15. Goswami G et al (2012) Face recognition captcha." 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications, and Systems (BTAS). IEEE
16. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol 14(1):4–20
17. Jain AK, Ross A, Pankanti S (2006) Biometrics: a tool for information security. IEEE Trans Inform Forensics Secur 1(2):125–143
18. Kelly, et al (1970) Visual identification of people by computer. No. CS-168. Stanford University, Calif Dept of Computer Science
19. Kim Y, Yoo J-H, Choi K (2011) A motion and similarity-based fake detection method for biometric face recognition systems. IEEE Trans Consum Electron 57(2):756–762
20. Kim W, Suh S, Han J-J (2015) Face liveness detection from a single image via diffusion speed model. IEEE Trans Image Process 24(8):2456–2465
21. Kollreider K, Fronthaler H, Faraj MI, Bigun J (2007) Real-time face detection and motion analysis with application in “liveness” assessment. IEEE Trans Inform Forensics Secur 2(3):548–558
22. Korshunov P et al (2016) Overview of BTAS 2016 speaker anti-spoofing competition. 2016 IEEE 8th international conference on biometrics theory, applications, and systems (BTAS). IEEE
23. Le C et al (2009) A survey of biometrics security systems. EEUU. Washington University in St. Louis
24. Lyu et al (2006) Steganalysis using higher-order image statistics. IEEE Trans Inform Forensics Secur 1(1): 111–119
25. Maltoni D et al (2009) Handbook of fingerprint recognition. Springer Science & Business Media
26. Marcel S et al (2014) Li. Handbook of biometric anti-spoofing, vol 1. Springer, New York
27. Marcel S et al (2014) Handbook of biometric anti-spoofing, vol 1. Springer, New York
28. Marcialis S et al (2009) Liveness detection competition 2009. Biometric Technol Today 17(3):7–9
29. Nguyen MH et al (2008) Image-based shaving. Computer graphics forum. Vol. 27. No. 2. Blackwell Publishing Ltd, Oxford
30. O'Brien J 2013 The scientific Sherlock Holmes: cracking the case with science and forensics. Oxford University Press

31. Pan G et al (2007) Eyeblink-based anti-spoofing in face recognition from a generic web camera. 2007 IEEE 11th International Conference on Computer Vision. IEEE
32. Phillips PJ et al. (2003.) Face recognition vendor test (FRVT) 2002: Overview and summary." Online: http://www.rvt.Org/FRVT2002/documents.htm
33. Ravibabu V et al (2014) A vary approach to face veritable recognition mechanisms for Android mobile against spoofing. 2014 IEEE Int Confer Computational Intelligence and Computing Research. IEEE
34. Smith DF et al (2015) Binary watermarks: a practical method to address face recognition replay attacks on consumer mobile devices." IEEE International Conference on Identity, Security, and Behavior Analysis (ISBA 2015). IEEE
35. Sun W, Song Y, Chen C, Huang J, Kot AC (2020) Face spoofing detection based on local ternary label supervision in fully convolutional networks. IEEE Trans Inform Forensics Secur 15:3181–3196
36. Yambay D, et al (2012) LivDet 2011—Fingerprint liveness detection competition 2011. Biometrics (ICB), 2012 5th IAPR International Conference on. IEEE
37. Yambay D et al (2014) Livdet-iris 2013-iris liveness detection competition 2013. Biometrics (IJCB), 2014 IEEE International Joint Conference on. IEEE
38. Yambay D et al (2017) LivDet-Iris 2015-Iris Liveness Detection Competition 2015. 2017 IEEE International Conference on Identity, Security, and Behavior Analysis (ISBA). IEEE
39. Yambay D et al (2017) LivDet iris 2017—Iris liveness detection competition 2017." 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE
40. Yambay D et al (2018) LivDet 2017-Fingerprint Systems Liveness Detection Competition. 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). IEEE
41. Zhang D, Shu W (1999) Two novel characteristics in palmprint verification: datum point invariance and line feature matching. Pattern Recogn 32(4):691–702
42. Zhang Y, Shi D, Zhan X, Cao D, Zhu K, Li Z (2019) Slim-ResCNN: a deep residual convolutional neural network for fingerprint Liveness detection. IEEE Access 7:91476–91487

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

ADITYA BAKSHI received a B. Tech degree in computer science and engineering from Kurukshetra University, Haryana, India, in 2010, an M. Tech degree in computer science and engineering from the YMCA University of Science and Technology, Faridabad, India, in 2012. He is currently pursuing a Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Jammu and Kashmir, India, and an Assistant Professor in the School of Computer Science and Engineering, Lovely Professional University, Punjab, India. He is currently involved in research work on biometric security and manet applications. His research interests include the security of next-generation biometric systems using image processing. Mr. Bakshi is a member of the International Association of Engineers and the Universal Association of Computer and Electronics Engineers.

SUNANDA GUPTA received the Bachelor's degree in Sciences and Master's degree in Computer Applications from the University of Jammu, and the Ph.D. degree in Computer Science and Engineering from Shri Mata Vaishno Devi University, Jammu and Kashmir, India, in 2014. She is currently an Assistant Professor in the Department of Computer Science & Engineering, Shri Mata Vaishno Devi University, Jammu and Kashmir, India with more than twelve years of teaching experience. She has authored several research articles in international journals of repute and presented papers in several international/ national conferences. She has also been invited as an expert to various international conferences as a reviewer/ technical program committee member. Her research interests include combinational optimization problems, genetic algorithms, and image processing.